REMARKS

Applicants appreciate the thorough review of the present application as reflected in the Office Action. Applicants have now amended Claims 1-6, 10-12, 20, 23-25, 29-40, and 45. Claims 7-9, 13-19, 26-28, 44, and 46 have been canceled. Applicants submit that all of the pending objections to the specification and claims have been overcome by the amendments herein, and that the claims are patentable over the cited references for the reasons discussed below.

Objections to the Specification

The Office Action has objected to the use of the acronym "DOS" as referring to "denial of service" on the grounds that "it stands for Disk Operating System (Microsoft Computer Dictionary, 5th Ed., page 173) ... [and that] the accepted acronym for denial of service is DoS with a lower case 0". (Office Action, Page 2). Applicants have not amended the Specification as suggested by the Office Action because Applicants, acting as their own lexicographers, have expressly defined "DOS" to mean "denial of service" and have consistently used that acronym throughout the Specification to have that meaning. (*See* Specification, Page 1, lines 9-10).

The tense of the verb "forward" has been corrected to recite "forwarded" by the above amendment to the paragraph on page 22, lines 12-22.

Accordingly, Applicants respectfully request withdrawal of the objections to the Specification.

Objections to the Claims

The amendment of Claims 20, 23, and 24 to depend from Claim 1 has overcome the objections to these claims.

The amendment of Claim 31 to recite a singular "storage device" throughout has overcome the objection to this claim.

The amendment of Claim 34 to recite a singular "IP address" has overcome the objection to this claim.

The amendment of Claim 37 to recite "a MAC address" has overcome the objection to this claim.

Accordingly, Applicants respectfully request withdrawal of the objections to the claims.

Rejections under 35 U.S.C. § 112

Cancellation of Claim 26 has rendered moot the rejection under 35 U.S.C. § 112, first paragraph.

Rejections under 35 U.S.C. § 101

Claims 32-34 and 37-39 stand rejected under 35 U.S.C. § 101, first paragraph, on the stated basis that "is it not possible for a spoofed source IP address to be bound to the MAC address of ... source devices." (Office Action, Page 4). Claims 32-34 and 37-39 have been amended to recite a singular address in the recitation of "spoofed IP address bound to the MAC address of the source device." Applicants submit that the rejections under 35 U.S.C. § 101, first paragraph, have been overcome by these amendments and, therefore, request withdrawal thereof.

Amended Independent Claims 1, 40, and 45 are Not Anticipated by Sharma et al.

Claims 1-12, 19, 26-28, 31, 33, and 40-46 stand rejected as anticipated under 35 U.S.C. § 102(e) by United States Patent No. 6,754,716 to Sharma et al. (hereinafter "Sharma").

Claim 1 has been amended to include the recitations of Claims 7-9, and independent Claims 40 and 45 have been similarly amended to emphasize the distinctions between the independent claims and Sharma. In particular amended Claim 1 now recites (emphasis added):

> 1. (Currently Amended) A method of determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:
>
> evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet; and
>
> determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address,
>
> wherein evaluating a source MAC address of the packet and the source IP address further comprises:
>
> identifying an entry in an address resolution protocol (ARP) table corresponding to the source MAC address;
>
> comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address;

> identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address;
>
> sending an ARP request to the source IP address if no entry in the ARP table is identified as corresponding to the source MAC address; and
>
> incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request.

Accordingly, the method of Claim 1 determines if a packet has a spoofed source IP address. A source MAC address and source IP address of the packet are evaluated by identifying an entry in an ARP table that corresponds to the MAC address, and determining if the IP address of the identified entry corresponds to the source IP address. The source IP address of the packet is determined to be spoofed when the source IP address of the identified entry does not correspond to the source IP address. An ARP request is sent to the source IP address if no entry corresponding to the MAC address is identified in the ARP table. If a response is received to the ARP request, it is incorporated into the ARP table as an entry corresponding to the MAC address.

In contrast, Sharma is directed to restricting what devices on a network can use ARP to discover the identity of other devices. In particular, "network devices are restricted from providing their network addresses to other than previously authorized devices." (Sharma, Col. 2, lines 4-6). The Office Action cites to Cols. 2 and 5 of Sharma as anticipating original Claim 1, however, that portion of Sharma is only describing embodiments of the ARP authorization process. Sharma describes that each of the network devices stores a list of IP addresses of devices that are authorized to determine via ARP the L2 address of the network device. (Sharma, Col. 2, lines 22-26 and 30-33). The list of authorized devices is loaded by each network device upon start up, and may be updated by a system administrator to reflect newly authorized devices. (Sharma, Col. 2, lines 33-37). Upon receiving an ARP request, the network device only replies back with its L2 address if the received source IP address is in the authorization table. (Sharma, Col. 2, lines 37-47). Sharma explains that "this prevents the first network device from discovering the L2 address of the second network device, and thereby directing any packets to it." (Sharma, Col. 2, lines 49-51).

Accordingly, Sharma is directed to restricting when a network device will respond to an ARP request using an authorized device table. It does not disclose a method of determining if a packet has a spoofed source Internet Protocol (IP) address. Moreover, the authorization table of Sharma is not an ARP table, and Sharma does not disclose that a source MAC address and source IP address of a packet are evaluated to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet by identifying an entry in an ARP table that corresponds to the MAC address and determining if the IP address of the identified entry corresponds to the source IP address. Moreover, Sharma does not disclose that a source IP address of a packet is determined to be spoofed when the source IP address of the identified entry from the ARP table dos not correspond to the source IP address.

Sharma also does not disclose the ARP discovery process of Claim 1 in which an ARP request is sent to a source IP address if no entry corresponding to the MAC address is identified in the ARP table, or that if a response is received to the ARP request it is incorporated into the ARP table as an entry corresponding to the MAC address. Instead, as explained above, Sharma describes that the list of authorized devices is updated by a system administrator to reflect newly authorized devices.

For at least these reasons, Applicants submit that Sharma does not anticipate Claim 1. Applicants request that if the rejection of Claim 1 is maintained that the Examiner provide Applicants with detailed citations of where the description of Sharma is contended to disclose every recitation of the claimed method.

Independent Claims 40 and 45 are system and computer program product claims that correspond to the method of Claim 1, and are submitted to not be anticipated by Sharma for at least the reasons explained above for Claim 1.

The dependent claims are submitted to be patentable at least per the patentability of the independent claims from which they depend.

Moreover, these claims are submitted to provide independent grounds for patentability. For example, Claim 2 recites:

> 2. (Currently Amended) The method of Claim 1, wherein determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address further comprises determining that the source IP address is spoofed

if the source IP address is not bound to the source MAC address **and the source MAC address is not associated with a gateway routing device**.

The Office Action rejects Claim 2 on the grounds that "Sharma teaches that the MAC address is associated with a router." (Office Action, Page 5). However, nowhere does Sharma disclose that a source IP address is determined to be spoofed if the source IP address is not bound to the source MAC address and the source MAC address is not associated with a gateway routing device. For at least these reasons, Applicants submit that Sharma does not anticipate Claim 2.

Amended Claim 30 recites:

30. (Currently Amended) The method of Claim 1, further comprising notifying a system administrator of a subnet of the source device and the presence of a spoofed source IP address in a packet from the source device when no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

The Office Action rejects Claim 30 on the grounds that "Sharma teaches discarding the packet if the source IP address cannot be resolved to the source MAC address at the source device." (Office Action, Page 6). However, nowhere does Sharma disclose that a system administrator is notified of a subnet of the source device and the presence of a spoofed source IP address in a packet from the source device when no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address. For at least these reasons, Applicants submit that Sharma does not anticipate Claim 30.

Amended Claim 31 recites:

31. (Currently Amended) The method of Claim 11, wherein a destination device of the packet comprises a network attached storage device and wherein discarding the packet if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address is carried out so that the packet is not forwarded to an Internet Protocol (IP) layer of the network attached storage device so as to increase the availability of the network attached storage device in the event of a denial of service attack.

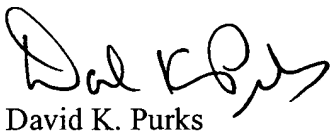
The Office Action rejects Claim 31 on the same grounds as Claim 30. However, the cited portion of Sharma discloses that if no correspondence is found between an ARP request and a table of authorized devices, the network device does not reply. Nowhere does Sharma disclose

that, when there is no entry the ARP table corresponding to the MAC address, a packet is discarded so that it is not forwarded to an Internet Protocol (IP) layer of the network attached storage device so as to increase the availability of the network attached storage device in the event of a denial of service attack. For at least these reasons, Applicants submit that Sharma does not anticipate Claim 31.

Conclusion

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

Respectfully submitted,



David K. Purks
Registration No. 40,133

Customer No. 46589
Myers Bigel Sibley & Sajovec
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401